PATENT
Docket No. 43521-0700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Examiner: TBD
Hidema Tanaka et al.	Group Art Unit: TBD
Serial No.: 10/622,722	
Filed: July 18, 2003	April 14, 2004
For: CIPHER STRENGTH ESTIMATING DEVICE	Irvine, California 92614

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In an attempt to fully comply with the duty of disclosure set forth in 37 C.F.R. § 1.56 and in conformance with 37 C.F.R. §§ 1.97 (b)(3) and 1.98, applicant wishes to bring to the attention of the U.S. Patent Office the following references:

> L. Knudsen, "Truncated and Higher Order Differentials," *Fast Software Encryption: 2nd International Workshop*, Leuven, Belgium (December 14-16, 1994), LNCS 1008, pp. 196-211, Springer-Verlag.
>
> X. Lai, "Higher Order Derivatives and Differentia Cryptanalysis," R^3 Security Engineering AG Ch-8607 Aathal, Switzerland, pp. 1-7; Reprint of pp. 227-233, "Communications and Cryptography," (Ed. R Blahut et al.), Kluwer Academic Publishers (1994).
>
> M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Fast Software Encryption: 3rd International Workshop*, Cambridge, UK (February 21-23, 1996), LNCS. 1039, pp. 205-218.
>
> S. Moriai, T. Shimoyama, T. Kaneko, "Higher Order Differential Attack of a CAST Cipher, *Fast Software Encryption: 4th International Workshop*, LNCS 1372, pp. 17-31.

A copy of these references and form PTO-A820 are attached.

If the Examiner believes that a telephone conference would help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

The Director is authorized to charge Deposit Account No. 19-2814 any filing fees which may be required.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 14, 2004, 2004.

By: James Lee

Signature

Dated: April 14, 2004

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920

Sheet 1 of 1

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney's Docket No. **43521-0700**	Application No. **10/622,722**
	Applicant **Tanaka et al.**	
	Filing Date **July 18, 2003**	Group Art Unit TBD

U.S. Patent Documents

Examiner Initial	Desig. ID	Patent Number	Issue Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
		L. Knudsen, "Truncated and Higher Order Differentials," *Fast Software Encryption: 2nd International Workshop*, Leuven, Belgium (December 14-16, 1994), LNCS 1008, pp. 196-211, Springer-Verlag.
		X. Lai, "Higher Order Derivatives and Differentia Cryptanalysis," R^3 Security Engineering AG Ch-8607 Aathal, Switzerland, pp. 1-7; Reprint of pp. 227-233, "Communications and Cryptography," (Ed. R Blahut et al.), Kluwer Academic Publishers (1994).
		M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Fast Software Encryption*: *3rd International Workshop*, Cambridge, UK (February 21-23, 1996), LNCS. 1039, pp. 205-218.
		S. Moriai, T. Shimoyama, T. Kaneko, "Higher Order Differential Attack of a CAST Cipher, *Fast Software Encryption: 4th International Workshop*, LNCS 1372, pp. 17-31.

Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	